NEW CYBER CRIMES: phising, pharming, HACKING AND CRACKING

Gudin Faustino Rodríguez-Magariños
Doctor of Law

SP / DOCT / 3705

1. INTRODUCTION: A WORLD FACING THE CYBERSPACE.

The term "cyberspace" comes from William Gibson's novel *Neuromancer* [1]. The concept draws a new frontier, a new territory that tries to shelter all the information, communications and ideas. The events taking place on the Internet are not happening in countries where participants or servers are physically, but a place where its true meaning is projected [2].

Cyberspace consists of transactions, relationships and thought itself, which stretches like a standing wave in the web all our communications. This digital world is both everywhere and nowhere, but not where bodies live. We are facing a new cosmos [3] in which, in principle, all may enter without privilege or prejudice accorded by race, economic power, military force, or place of birth. a new open space where anyone, anywhere may express their beliefs, no matter how singular, without fear of being coerced into silence or conformity is set.

However, as holding L ESSIG [4], Cyberspace is not a place but many places and characteristics of each are not always identical, differing from each other in their most fundamental characteristics.

At first it was understood that cyberspace configured a territory that was essentially free, that it was not capable of being governed and therefore outside all control and resistant [5] against any domineering influence. so J OHNSON / P OST [6] They proclaimed that:

" *He has appeared a new electronic means indifferent to the geographical limits which produces confusion within the law by creating entirely new phenomena that need to become subject to clear legal rules but which can not be controlled, in a satisfactory manner, by any of the forms current sovereignty based on territoriality* ".

---

[1] Vine. G IBSON, William, *Neuromancer (* trad. Arconada, José), Planet, Barcelona 1996. Neuromante is the first novel of a composite trilogy also by Zero Count (1986) and Mona Lisa Overdrived, (1988). While they are sharing the same universe and some characters have little to do with each other. The title comes from the English word "Neuromancer" and arises from the composition of the terms; "Neuro" (mental) and "Mante" (subject or actor of "Mancia" which means divination and magic extension (eg Necromancer, quiromante)). Thus we have "Neuromancer" as a direct translation *Neuromancer.* Gibson's cyberspace is a cyber adventure camp jeans. It is illegal hackers getting information online on behalf of large corporations and to that end they move to Matrix.

[2] This O RTEGA G iménez states that "the fact that *Internet* or, if you will, "cyberspace" ignores borders, since all private relations with *Internet,* are transboundary, this is potentially international; second, *Internet* He wants the information it makes available to its users is free; third, *Internet* despite having become an unprecedented phenomenon, we must not forget that, in practice, it is nothing more than a technological environment; and a quarter, *Internet,* since its inception, it has made a major effort to be resistant to the regulation of states. "In" Internet regulation "[O RTEGA G Iménez, Alfonso, *Journal of Computer Law AlfaRedi. No. 061,* August 2003 http://www.alfa-redi.org/enlinea.shtml].

[3] The cosmos cyberspace tends to displace it as disinformation Grass says: "Only science and ignorance are linked in space and time". [Cf.. G RASS, Günther, op. cit, p. 227].

[4] Vine. L ESSIG, Lawrence, *Code and Other Laws of Cyberspace (* trad. Alberola, Ernesto), Madrid, 2001, p. 125.

[5] S and T TEINER- HRELKELD expresses "respect the Government of the network some things never change. Most notable is its ability to resist the government in any form ". [S TEINER- T HRELKELD, Tom, ["Of Governance and technology" *Inter @ ctive Week online,* October 2, 1998].

[6] Cfr. J OHNSON, David R. / P OST, David G., "Law and Borders-The Rise of Law in Cyberspace" *Stanford Law Reiew,* Vol. 48, 1996, p. 1367.

More as points L ESSIG [7] modernly these approaches tend to be reputed mere myths, giving way to a new more complex reality that reveal the existence of multiple architectures within the network to conceal the existence of numerous and diffuse interests [8].

Therefore, cyberspace has its own code or rules of conduct which interact netizens (*netizens)* apparently free but subject to a pre-set architecture. That hidden code as preached K ATSH [9] It stands as architect of his own environment [10].

The information society of the XXI century by great technological dependence of all citizens who are unable characterized each day to function more autarkic (*computer dependency).* The soul and backbone of this new company is projected internet in cyberspace a common space of globalized information. In fact it has even come to talk about a new evolutionary stage of man as either " *homo digitalis* "Or as" computerized ape ".

In cyberspace multitude of services that transform our customs, benefits are based on strong communication skills offered by the network are implemented. also treats services like tele-education (*e-learning),* electronic commerce (*e-commerce)* or electronic administration (*e-government),* telemedicine (*e-health),* Electronic Enterprise Resource Management (*e-management),* telematics banking (*home-banking)* [eleven], teleworking (*tele-work),* the advertising offer (*cybermarketing)* or more directly in the area of managing domestic sphere (domotics).

Such is the heritage field expansion is occurring in cyberspace, we must ask whether e-commerce appears as the manifestation of a *New Lex Mercatoria International* [12] or if, reaching even further, international trade will be fully absorbed by e-commerce.

But these new features are only isolated manifestations of a larger phenomenon that arises how multi-arm squid everywhere. The digitization of the network, the stored post-program monitoring, fiber optic synchronous digital transmission of high-speed, integrated management systems and many other technologies and improvements appear continuous, allow the emergence of new services that are being incorporated gradually market and enable a qualitative leap in communications.

Cyberspace is a place where it is, in principle, all feasible communication with everyone, anywhere and with the ability to transport bidirectional audio, visual information, text and graphics. The infosphere tends to expand their domains to any public or private information: police, judicial, banking, bureaucratic, commercial, medical, military, financial, tax, registration, etc.

By sheer inertia all our technical data flows and incessant repetitively over the network, the domain of cyberspace feeds and takes shape gradually as omniscient. As the

---

[7] Vine. L ESSIG, Lawrence, op. cit., p. 67.

[8] Taken by reference G arcia M exia, Paul, *Principles of Internet Law,* Tirant lo Blanch, Valencia, 2002, p. 99. In the same vein, John P. Barlow made in 1990 the Declaration of Independence of Cyberspace in proclaiming: "In cyberspace we have no elected government, nor is it likely to have, which is why I address you, Governments industrialized world with no more authority than freedom itself speaks. I declare the global social space we are building is by nature independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods to make us fear your law, we should truly fulfill. You have no moral right to rule us nor do you possess any methods to make us fear your law, we should truly fulfill. Your legal concepts of property, expression, right to identity, freedom of movement and context do not apply to us. They are based on matter. Here in cyberspace there is no matter " .

[9] Vine. K ATSH, Ethan M., *Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace,* Chicago, 1996, pp. 335-360.

[10] and M ITCHELL He states that, contrary to what is believed, cyberspace is not a chaotic place but as happens in space requires some supports or structures. So the author argues: *"Architecture, laws and customs maintain and represent any existing balance in real space. As it builds and widens scope tends to create and maintain a similar balance, although these will be embodied in software structures and electronic access controls rather than architectural type arrangements* ". Cfr. M ITCHELL, William J., *City of bits: Space Place and the Infobahn,* Cambridge, Massachusetts, 1996, p. 159.

[eleven] A new dimension is the possibility of certain financial institutions to issue electronic money, a possibility that appears regulated by Royal Decree 322/2008 of 29 February (BOE no. 54 of 3DE March 2008) on the legal status of entities electronic money.

[12] Thus C ALVO C ARAVACA, Alfonso Luis / C ARRASCOSA G onzalez, Javier, "Internet, B2B international staff and Lex Mercatoria" *Journal of European Studies, no. 39,* 2005, pp. 105-116.

information a way to understand the power, cyberspace is placed as a new increasingly powerful body that tends to nullify the individual. More paradoxically, as noted M OLES [13], It corresponds to justice and the right task to avert the danger by which human beings can become defenseless and helpless against the telematic operators and regulators.

There is a legal right that is legal certainty (art. 9.3 CE) which extrapolates Internet security in cyberspace is as important in the face of a modern economy already beginning to emerge "cyber police" trained to handle these complex latitudes. In short, new values that generate new conflicts but the weight of the network in the world economy it is becoming increasingly accused.

As G says Omez M Artin [14], there can be no denying that the cyberworld program is a multifaceted reality with various aspects worthy of legal protection. But cyberspace with the possibilities of development and progress that involves humanity can be reputed as a legally worthy of greater protection.

2. phising

It is known as' *phishing* ' (of English *fishing,* fishing [fifteen]) the phishing (online, but also in other ways) which seeks to appropriate confidential data from users, based on them, get heritages undermine others. The crime is to obtain information such as credit card numbers, passwords, account information or other personal information by deception. This type of fraud is usually conducted through emails or pop-ups.

The SJPI of Murcia [16] defines this practice as a type of crime falls within the scope of the scams that translates into a telematic tactic by which the user is taken to a page "web" with appearance that is to your financial institution and is characterized by acquiring confidential information fraudulently (as may be a password or detailed information about credit cards or other bank information). The scammer, known as phisher is passed by a person or trust company in an apparent official communication electronics, usually an email, or any instant messaging system or even using also telephone calls. After obtaining these confidential data, *phiser* proceeds to seize the wealth of others ordering bank transfers.

The scam in classical Roman law was conceptualized as *stellionatus crime* [17] (Chameleon crimes) were as varied as the types of *modus operandi* it was hard cataloging difficult, and appeared clearer when described, the easier it evade its consequences by altering some of the variables or insitas premises in its definition. It seems an inescapable fact that scientific advances always go ahead of the law. This asynchrony between technology and law creates a legal vacuum which must be covered by the system so quickly, suffering "horror vacui" [18]. Given the growing number of reported phishing incidents related to additional methods of protection are required. Attempts have been made to laws that punish the practice, campaigns to prevent users and implementing technical measures to programs.

Etymologically, the term phishing comes [19] of the English word "fishing" [twenty] (fishing) referring to the act of fishing hooks users with increasingly sophisticated, and thus obtain

---

[13] Vine. M OLES, Ramon J. *Law and control of internet,* 1st Ed., Ariel, Barcelona, 2004, esp. pp. 17 to 21.

[14] Vine. G Omez M ARTIN, Victor, "The criminal protection of copyright on software: An example of the patrimonial nature of crimes against intellectual property in the CP 1995 (1)" *Review of the Judiciary. No. 66,* 2nd quarter 2002, p. 145.

[fifteen] The term phishing was adopted by crackers attempting to "fish" accounts anonymous victims; ph is commonly used by hackers to replace f as root ancient form of hacking known as "phone phreaking".

[16] SJPI Murcia, 69/2007, 30 March (RJ 2008/44072).

[17] Vine. M ENTXAKA E LEXPE, Rosa Maria, "Stellionatus" *Bullettino dell 'Istituto di Diritto Romano "Vittorio Scialoja, no. 30,* 1988, pp. 277-335.

[18] Vine. DER UGGIERO, Roberto, *Civil rights institutions,* 4th Ed. Italiana (Naples March 1915), (trad. Serrano Suner, José Santa- Cruz), Madrid, 1943, p. 163.

[19] The first mention of the term phishing data from January 1996 newsgroup alt.2600 hackers, although the term appeared early in the printed edition of "Newsletter hacker".

[twenty] Vine. D REYFUS, Hubert L., *About internet (* trad. Hormazábal, Cristian P.), EDIUOC, 1st Ed., Barcelona, 2003, pp. 112 et seq.

financial information and passwords. Another etymological version of the term "phishing" is found in the contraction of " *password harvesting fishing* "(Harvest and phishing), although probably only a retroactive acronym.

Most methods of phishing use some form of technical deception in the design to show a link in an e-mail seems a copy of the organization which is passed the impostor. The quality of the hook depends on the quality of *phiser* in all cases, the entity can measure the *criminis iter* made, as in scams usually always attend some negligence, more or less by the victim, and we must be on the subjective circumstances surrounding it.

In another popular method of phishing, the attacker uses against the victim's bank code or service which is passed program itself. This type of attack is particularly problematic because it directs the user to log on to the bank's own site or service where the URL and security certificates seem correct. In this method of attack (known as *Cross Site Scripting)* users receive a message saying they have to "verify" their accounts, followed by a link that looks like the real website; Actually, the link is modified to perform this attack, it is also very difficult to detect if they do not have the necessary knowledge.

One of the most important aspects is money laundering. Currently fictitious companies try to recruit teleworkers through e-mails, chats, IRC and other media, offering not just work from home but also other lucrative benefits. Those who accept the offer will automatically become victims who commit a serious crime without knowing it: the so-called "money laundering" obtained through fraudulent act of phishing twenty-one.

the so-called *spear phishing (* literally spear phishing) is one of the most recent attempts of phishing victims taking customers from banks and online payment services. Although the example shown in the first image is sent by phishers indiscriminately hoping to find a customer of the bank or service, recent studies show that phishers initially are able to establish what bank a potential victim relates, and thereby send an e-mail, falsified appropriately, the potential victim.

Another way to make the global phishing is by sending millions of emails under the guise of banks, requesting the keys to the bank account or specific attacks. The third step is that the scammers start to withdraw large sums of money, which are transmitted to the accounts of intermediaries (muleteers).

Intermediaries perform the transfer to the accounts of swindlers, taking these amounts of money and those intermediaries -the percentage of the commission.

In the United States, Senator Patrick Leahy introduced the Anti-Phishing Act 2005 on 1 March 2005. This federal law anti-phishing stated that those criminals who create fake web pages or send spam e-mail accounts with intent to defraud users could be fined up to $ 250,000 and imprisonment for a term of up to five years.

3. PHARMING

Pharming is the exploitation of a vulnerability in the software of the DNS (Domain Name System) servers or teams of users, which allows an attacker to redirect a domain name (*domain name)* to a different computer. Thus, a user to enter a

twenty-one For a person can register with this kind of companies you must fill out a form which will indicate, among other information, your bank account number. This is intended to enter the money from bank fraud made by the method of phishing on the account of the worker-victim. Once hired, the victim automatically becomes what is commonly known as mulero. With each fraudulent act *phishing* the victim receives substantial income in your bank account and the company notifies you of the fact. Upon receipt of this income, the victim a percentage of total money will stay, may be around 10% and 20% as a working committee and the rest resends through systems send money to accounts indicated by the pseudo- company. Given the ignorance of the victim (often motivated by economic necessity) it is involved in an act of important swindle, it may be required by justice on a complaint banks. These complaints are usually resolved by imposing return all money stolen from the victim, ignoring the fact that this only received a commission.

given domain name that has been redirected, will enter into your Internet browser to the website that the attacker has specified for that domain name.

The word *pharming* derived from the term "farm" (farm) and is related to the term "phishing", used to name the social engineering technique [22] that by spoofing emails or web pages, try to obtain confidential user information, from credit card numbers to passwords. The etymology of this word is that once the attacker has gained access to a DNS server and taken control of it, is as possessing a "farm" where pleasure can make use of the resources found there.

Pharming is based on the knowledge that the internet computers have a unique IP address, consisting of 4 octets (4 groups of 3 digits) from 0 to 255 separated by a period (eg
139.0.0.2). These IP addresses are comparable to postal addresses of the houses, or the number of phones. Because of the difficulty would users have to remember these IP addresses, emerged Domain Names, which are associated with IP addresses in the same way that people's names are associated with their telephone numbers in a phone book.

Exploits *pharming* They are often perpetrate in two ways: directly to the DNS servers, so that all users would be affected or attacking specific computers by modifying the file "hosts" present on any computer running under Microsoft Windows or Unix systems .

Technique *pharming* It is normally used for phishing attacks, redirecting the domain name of a trusted entity to a website, identical in appearance, but actually created by the attacker to get the private user data, usually bank details.

4. LEGAL STATUS

We can distinguish Instruction No. 4/2007 of the Chief Prosecutor of the Supreme Court in Madrid two aspects:

to) Phiser behavior or Phamer

As we know, *phiser* or *farmer* The person who goes to a web page (from a bank or an individual) and takes over the keys of access to electronic banking transfers nonconsensual making money at the expense of current accounts of victims.

This failure was evident in the STS of April 19, 1991 [2. 3], in which the conduct of a bank employee who handled the current accounts of several clients via computer and more than three million pesetas pocketed scored. The court found that there was no fraud, misappropriation but since there was no deception on the victims to take them to cause them the necessary error that induce them to make this heritage available for the perpetrator. The solution given by this ruling, considered doctrinally very forced, held in his FJ 2nd:

" *The "induction" an act of disposal of assets is realizable only against a person and not against a machine, involves a comisiva ideological dynamics charged substrate. Rightly it stressed that the machines do not they can be fooled, computers either, so the cases in which the damage occurs directly through the computer system with which operations transfer of assets perform, no deceit or error required for the crime of fraud occurs. Without deception, cardinal element con, not be understood produced this* ".

In fact since no actual deception to another certain sector of the doctrine shuns, inappropriate, the use of the term "scam" [24]. Therefore, one of the main features of computer scam is that structurally is not required deception, because as argued STS 20

---

[22] If we look in a dictionary of English the term pharming, we will find it defined as " *production of drugs from plants and animals genetically altered ".* At a conference organized by the Anti-Phishing Working Group, Phillip HallamBaker defined this term as "a marketing neologism designed to convince bankers and businessmen to buy new equipment or safety accessories."

[2. 3] STS 191 April 1991 (Soto Nieto) [RJ 1991/2813].

[24] And M unoz C ONDE, Francisco, *Criminal law. special part,* 15th Ed, Tirant lo Blanch, Valencia, 2004, p. 426.

November 2001 [25], Since we are in a committed fraud through a transfer without consent by the victim through computer manipulation, it is not necessary the concurrence of any deception by the scammer. This is so because the ambuscade to foreign assets through computer manipulations performed acts with automatic detriment of third, precisely because there is a computer manipulation and deception so the staff is not required.

After the reform of LO 15/2003 a third section for, advancing the barrier punitive, punishing the manufacture, introduction, possession or facilitation of computer programs specifically aimed at the commission of common scams or computer is introduced. As well holds M unoz C ONDE [26], such conduct would not pass from being mere unpunished preparatory acts and the guardrail in response to the important role of information technology in modern traffic comes forward though, seems a bit much his punishment with the same penalty as a crime abstract.

Instruction No. 4/2007 of the Chief Prosecutor of Madrid distinguishes the following assumptions:

1) Misrepresentation of the website to obtain access codes and passwords and use of the so obtained to take money from current accounts by bank transfer. Chief Prosecutor Madrid (Manuel Moix) urges prosecutors to pursue this type of behavior as a crime of computer fraud Art. 248. 2 CP and a crime against privacy of art. 197.2 of the Penal Code. However because what happens alleged contest rules (art. 8.1 of the CP) are encouraged to qualify exclusively as a computer fraud (Art. 248.2 CP).

As noted by the aforementioned STS of 20 November 2001 argues the need for a special type for this swindle:

" *The Criminal Code of 1995 introduced paragraph 2 of art. 248 Criminal Code a specific type of fraud to establish acts acechanza to assets outside made by performing manipulations and devices that do not address other, but machines whereby it, as a result of devious behavior, acts in automatism detriment of third parties. These assumptions do not fit in the previous understanding of the scam because the author did not fool another but a machine. In the trial course, the use of a credit card pretending to be the owner could not be integrated into the classic concept of the scam as the "deception" was made to the machine automatically it effected the financial arrangement.* ".

2) Misrepresentation of the website to obtain key page and access passwords without, transfers, then the sale or transfer of these keys and passwords is done. In this case the prosecutor Madrid understands that we have a crime of divulging secrets of art. 197. 2 and 3 of CP.

3) Misrepresentation of a website to obtain keys and passwords for access and use only part of the thus obtained to draw down money from current accounts by bank transfer, preserving the rest or transmitting them to a third party: it will qualify as a crime art computer fraud. 248.2 CP and other revealing secrets of art. 197.2 and 3 of the CP in real competition.

b) Conduct "mulero"

As for the conduct of "mulero" (person who opens or "lend" its current account for the phiser make money income of the victims, usually by a division of the spoils, either a lump sum or through a fee or percentage. it is not unpunished and qualify, depending on the case, or as a crime of computer fraud Art. 248.2 CP (STS 533/2007 [27], 12 June) or as an offense of money laundering Art. CP 301, considering the circumstances, singularly the origin of the money.

5. ELEMENTS OF ciberestafa

[25] STS 2175/2001 (2nd), 20 November (Martinez Arrieta) [RJ 2002/805].
[26] Vine. M unoz C ONDE, Francisco, op. cit., p. 426.
[27] STS 533/2007 (2nd, Sec. 1st), 12 June (Giménez García) [RJ 2007/3537].

The main constituent elements are:

- The Profit: refers to the subject act with desire or intention to enrich themselves, to increase their assets, if any, to circumvent a debt.

- The typical action is to rely on a computer or similar device. After the reform of LO 15/2003, of 25 November, the concepts of "deceit and error rather" being replaced by "tamper" disappears. It corresponds to the behavior to alter, modify or hide computer data so that operations incorrectly made or not carried out, and also with behavior change program instructions in order to alter the outcome that expected. Thus a subject can enter incorrect instructions in an accounting program so that no record charges to your checking account for example, or to move to your bank account all income made a certain day to accounts whose numbers end in particular.

The reference to "any computer or similar device" seems able to accommodate all possible cases through an unauthorized transfer of property assets to the detriment of a third party is made, either in making program modifications or alterations in processing, and in manipulations input, output or data transmission. As noted, the legal formula is very wide, although perhaps inevitable in this field, in which technological development is ongoing, with the danger that a stricter prose leave soon obsolete provision [28]. The reference to "similar device" might suggest that other non-computer nature maneuvers are also included. However, the meaning of paragraph obliges him understand that everything is based on these assumptions, so the legal mention must also be interpreted from that perspective.

- Involuntary transfer of the assets of another person without using violence. What is usually translated into a shift of money from the victim's bank account to the account of the offender.

- Subject to third, since it is not the victim who performs economic transfer, but is the author of the crime which takes place.

Regarding the subjective element of the unjust, this crime does not fit the culpable commission, the perpetrator acts willfully, that is, knowing and wanting to perform acts of criminal action. The concept of "computer manipulation" itself implies intentionality of the active subject; is difficult for anyone to carry out acts of alteration, modification of data or software error and also will report an economic benefit, because these actions require knowledge of the data or correct instructions and replace them with others, the subject knows that his performance It constitutes an action contrary to law and still is carried out.

6. HACKING

He *hacking* or computer intrusion, consisting unauthorized access [29], usually violating security mechanisms where they exist, files and databases contained in the foreign computer systems, typically large companies or institutions.

He *hacker* It appears in certain environments amateur surfers, with some fictional aura, tinged with some consideration and respect, given its expertise to skip the barriers or safety devices frequently greatly entangled with which computer systems are shielded and bases information banks, state military institutions or large companies and multinationals, sometimes even computer. Rush *hacker* They are retraced as a kind of modern computer version of the myth of Robin Hood [30] (or David

[28] Vine. Q UINTERO O LIVARES, *Comments to the special criminal law,* Aranzadi, Pamplona, 1996, p. 491.

[29] You can give access to passwords by "bugs" or through Trojans or programs that help decipher the word or password when dialing. Examples of programs commonly used for such actions are Subseven or Netbus, which are small applications configured by the programmer or commonly used and cracked by hackers.

[30] This syndrome of "Robin Hood", involves a "parallel moral" that is said to be immoral damage done to specific individuals, but not caused to organizations or companies (Vid. S ARZANA, Carlos, "criminalità and technology: Il caso dei computer-crimes" *Rassegna Prison and Criminological, nos. 1 - 2,* Year 1. Rome, 1979, p. 74). Very often the means used are not considered illegal in the computing environment (illegal copies of programs, unauthorized exchanges of programs,

vs. Goliath), but the truth is that behaviors *hacking,* although in itself need not be harmful, because once circumvented the protective barriers computing the *hacker* usually leave the system without ulterior motives, it remains true that, on many occasions, are the prelude to serious violations of privacy, the rights of intellectual property or against company secrets.

Criminal offense, where the *hacker* is limited, without more, to meddle is very confusing, because if the behavior continues in the strict field of computer intrusion, must be considered from the point of view of criminal relevance, such as impunity or atypical. Moreover, even reaches the consideration of an attempt or a preparatory measure (where this was punishable) because the subjective element is not fulfilled, since the purpose of *hacker* not infringe privacy or intellectual property against nor is damage systems or software in which it intrudes.

In this sense, pronounced the Order of 29 January 2002 the Court of Instruction No. 2 of Lorca [31]
destipifica behaviors that considering that not fulfilled the subjective element of the unjust and declaring in his FJ 2nd:

"Hacking behaviors mere access to computer systems perpetrated with the sole purpose of accessing the password or NAND logic gate They are currently constitute a crime because they lack the subjective element of the unjust. "

From the point of view of criminal policy, this absence of criminal relevance is severely criticized by some sectors who do not hesitate to consider the *hacking* You should have a specific offense.

The most common manipulations are typically produced by the introduction of false data, alteration of the programs or the use of logic bombs, Trojan horses, and analyzed, or techniques such as salami [32], causing the automatic execution of bank transfers, income or credit recognition in favor of the person making the alteration [33]. The average employee and

---

introduced into computer systems for fun, use the system for their own purposes, etc.), whereas at most such behaviors may be "irregular", perhaps a simple "game" or "hobby" but in any case illegal (vid . G US onzalez R, Juan José, "Approaching the criminal treatment of illegal property with computer means or procedures" *Journal of the Faculty of Law at the Complutense University, Num. 12* 1986 pp. 110-111; C L OSA Camacho, C Camacho L OSA, Luis, *Cybercrime,* Madrid, Charts Condor, 1987, pp. 74 ff .; G UTIÉRREZ F Rances, Maria Luz, *computer fraud and fraud,* Publications Center Ministry of Justice, Madrid, 1991, pp. 74 et seq.). Contrary to popular belief, it is accurate or superior intelligence in the author nor high technical knowledge is required, but is capable of being developed behavior by any minimally introduced in the management of information technology. Known cases of young people who, almost like a game, are introduced into sophisticated computer systems is more than significant proof of this. According to studies carried out in relation to the known cases in the United States and West Germany, the authors are usually young people (between 24 and 35 years), educated, mostly male, with no criminal record, awake, very active, eager and highly motivated, They are acting for various reasons (revenge, profit, Carlos, op. cit., pp. 76-77).

[31] Alcázar Ponente Fajardo.

[32] This name to input instructions to transfer own accounts resulting accumulation of cents that are ignored when operating with current account, interest calculation, amounts, financial transactions, etc., and reaching significant amounts (vid., C Camacho L OSA, Luis, op. cit. ,, pp. 41-42 and S Neyers, Alfredo, *Fraud and other cyber crimes,*

Management and Production Technologies, SA, Madrid, 1990, p. 112).

[33] Manipulations may occur at any time of the processing of data or system operation. In the input phase data, for example, by introducing false data (providers or fictitious shareholders, false bills lacking employees, erroneous wages, etc.) so that the computer automatically without manipulation in the program, performs fraudulent operation (dividend payment, bank transfers, payroll calculation, etc.). Manipulations in the program require alteration of statements and instructions of it to carry out operations other than originally intended (sentences that add cents to the price of products and transferred to own accounts, instructions for modifying inventory and subtract items stores, forwarding to own accounts of the remains in the calculation of interest, etc.). They are often accompanied by changes in the output data, so changes are not reflected in the lists or accounting (assigning them to false starts, omitting operations, etc.), making it difficult, so the discovery of the fact. In connection with data transmission networks or running in short interfering transmissions, illegitimately accessing the system to discover confidential information, modify files, perform fraud, etc. Sample input manipulations in the case of those who work in the Department of Family Allowances Working in an office and over nine months to transfer commands fictitious family allowances for children to various bank accounts, being discovered by chance. Modification example in the case of programs who enter the program data introduces several fictitious payroll employees whose salaries were to be paid to own accounts. It also modifies the program that generates the lists of salaries, accounting reports and balance sheets for those employees nor the amounts allegedly paid to them, it follows, that is not reflected in accounting, account tax not appear detracted to rent

acting with and on machines and not on people, along with the fact that the use and affects behavior in incorporeal elements are the defining characteristics of these assumptions and that give them identity from the criminal point of view.

However, concern about its development explains why it has been expressly typing in some jurisdictions [3. 4.] Not so in the Spanish penal code, which contains no provision generically punish unauthorized access to computer systems of others. As a result, the punishment of these behaviors will only be possible to the extent that they will refer to data that are subject to special protection or involve behaviors that are includable in criminal generic types.

Quite the contrary consider that there is insufficient regulation administrative regulations to deal with such situations and responsibility servers not take appropriate technical measures to restrict such abuse.

The most serious problem is the incardinación most hacking behavior in the repressive criminal law.

If the purpose is to discover the intimacies of a particular concrete it seems to be perfectly incardinables in the art. 197 CP. The problem arises when there is not a random relationship between victim and hacker Incardination less conflicting results when, due to the selective and restrictive function of the subjective element of the unjust.

Authors such as M ORAL P RATS [35] however understand that most cyberbullying behaviors or freedom or against computer *privacy* They should be subsumed in the art. CP 197.2 (lacking the subjective element of the unjust paragraph 1).

When the volitional element is aimed at discovering the "trade secrets" such conduct would be protected in the art. 278.1, which is the basic reference of these behaviors: "Whoever, to discover a secret company seizes by any means of data, written or electronic documents, computer media or other objects relating thereto, or uses any of the means or instruments referred to in paragraph 1 of Article 197 ' [36].

The provision expressly refers to 'data, documents ... electronic, computer media ... "and for forwarding to 197" emails ... telecommunications ... or ... any other signal

---

workers (Vid., by all T IEDEMANN, Klaus, *Economic power and crime (* trad. Matilla Villegas, Amelia), Ariel, Barcelona, 1985, pp. 124-25 and S ieber, Ulrich, "Documentation for an approach to computer crime" *Cybercrime,* op. cit., pp. 68 et seq.). Entering data or program modifications can be produced directly in the computer system that handles the author or another that is accessed without authorization.

[3. 4] Thus, § 202 StGB (Espionage data): "Whoever without authorization try himself or other specially secured data against unlawful interference" (imprisonment of up to three years or a fine). For this purpose, data are considered "only those electronic, magnetic or stored in a manner not immediately perceptible or which are transmitted" (vid., M ÖHRENSCHLAGER, Manfred, "Trends in legal policy in the fight against cybercrime" *computer crime (* coord. Mir Puig, Santiago), Ed. PPU, Barcelona, 1992, pp. 60-61 and "The new computer criminal law in Germany" *Informátic crime* a, op. cit., pp. 135-138). Similarly, art. 615-ter of the Italian penal code "abusive access to a computer or telematic system): The abusively is inserted into a computer or telematic system protected by security measures or kept in it against the express wishes or tacit who has the right to exclude him, it shall be punished with imprisonment of up to three years. "; penalty will be aggravated, among other things, whether the destruction or damage to the system or the complete or partial interruption of its operation or damage data, information or programs on the same content is derived from access. Beyond what is ordinary in the punishment of computer-related behaviors, art. *Profili penali dell'informatica,* Giuffre, Milan, 1994, pp. 28 et seq.).

[35] Vine. ORAL M P RATS, Firmin, *Comments on the New Penal Code,* Aranzadi, 4th Ed., Pamplona, 2005, p. 1063. Thus the author argues: "In this way, the behavior interception, recording or electronic reproduction illicit computer communications (emails), for example, violating the" password "or re-access key should be subsumed in the second typical sequence art. 197.1 of the Penal Code ". These behaviors would also be typified whether the acquisition had taken place on the screen as if it were done on computer correspondence and printed outside the system.

[36] If in addition to discover the secret, the subject it disseminates, revelare or intends to transfer to third parties shall apply art. 278.2. Where these behaviors are performed by those who have legal or contractual obligation to maintain confidentiality, the art must be taken into account. 279. And if the facts are effected by who was not involved in the discovery, but he knows the secret illicit origin of the company, the provision will be callable art. 280. For further study of the same vine. G onzalez R US, Juan José, *Course of criminal law,* Vol. I, cit., Pp. 796 et seq.

communication ", which places him squarely within the assumptions we try to the extent that the" empowerment "of them represents in itself a unauthorized system or computer where they are accessible.

For jurisprudence does not seem to be a decisive element relevance of data seized, and the STS of June 11, 2004 [37] condemns an official INEM seizes merely references related to the workplace and address of the company regarding a database belonging to the General Treasury of the Social Security.

it does not seem possible, because it would be too forced, incardinar behavior in article 256 of the CP as does any sector of the doctrine, arguing that rely surreptitiously apparatus and connected as the diction of the type seems to be oriented so-called theft of Use computer time or unauthorized use or overstepping it. In turn, as noted V ALLE M UNIZ / Q UINTERO

OR LIVARES [38], the draft Penal Code demanded a "surreptitious" use, typical element which was already despised in processing paper.

Given the legal loophole failure and no shortage of authors [39] advocating an advancement of punitive barrier (creating obstacles or barriers crimes as happened in France) and Based n to illicit committed frequently in the so-called dark area of cyberspace are often the prelude to other major illicit, since the hacker rarely content to smooth the digital space of the citizen concerned and tends to manifest their intromisivo power committing other new transgressions.

7. - CRACKING

Also known as computer sabotage. We must not confuse it with the *password cracking* or breaking or decryption key (*passwords)* which is similar to *hacking.* In the first direction, M ARCHENA [40] defined as consisting of the destruction or widespread damage output on your system, data, computer programs or data transmission behavior.

But as stand M ATA Y M Artin [41], The main thing about this kind of behavior is that are aimed at attacking the logical elements of the system, ie the software in general and files or computer files in which data, information or documents are collected, whatever their specific content . As the doctrine review [42], he *modus operandi* concrete (deletion, formatting, virus) is indifferent.

Among the most serious behaviors, it is remarkable, behavior *cyberpunker* or *cyberpunking,* which can be translated into Castilian as electronic vandalism or computer sabotage, by which the perpetrator is dedicated to delete, delete or modify, without the consent of the holder, functions or data from a computer with the intent to hinder normal operation. The forms through which this behavior is carried out are, from the point of view of logic operation of computer systems and mechanisms, varied and normally, from the point of view of terminology, all are unified by reference to infection by computer virus systems.

Lately some peculiarity charges *smurfing* consisting of where Storming is the network router or *router,* overburdening the service through continuous massive attacks using slave systems or attack the system with a large number of packets with false IP addresses (*flooding),*

blocking the system and causing global denial of service (*DdoS* or *Denial of Service).*

Sometimes known as viral advertising or viral marketing (*pop ups)* It can be incardinable in this, when as a result of these practices at least as a possible fraud it is expected that it will result in a inconsentida installation involving damage to the affected computer operating systems.

---

[37] STS (2nd) of 11 June 2004 (Bacigalupo Zapater).

[38] Vine. V M UNIZ ALLE, Jose Manuel / Q UINTERO O LIVARES, Gonzalo, *Comments on the New Criminal Code,* op. cit., p. 1307.

[39] Vine. M ORON L ERMA, Esther, op. cit., p.75.

[40] Cfr. M ARCHENA G Omez, Manuel, "The computer sabotage: offenses between damage and public disorder" *Current Legal Aranzadi, no. 40,* July 2001, p. 7.

[41] Vine. M ATA YM ARTIN, Ricardo, *computer crime and criminal law,* Edisofer, Madrid, 2001, p. 59.

[42] Vine. P ynol R odríguez, Jose Ramon, *Manual of Criminal Law. Part. Special,* 4th Ed, Thomson Civitas, 2006, p. 293.

As we saw, the *cracking* It is therefore a concept computer nonmaterial [43], because the data included in the physical media directed to hardware or computer medium whose damage must be sheltered in the generic type of damage (Art. 263 to 625 crime and lack). For criminal prosecution of computer sabotage has created a specific type of art. 264.2 of the Criminal Code that would shelter damage to data provided for in art. 4 cybercriminality Convention. Although the opinion of a certain sector of the doctrine [44] such as typing was not essential they appeared already protected in the generic offense of damage.

As regards C REMADES G arcia [45] in the exegesis of this art. 264.2 is necessary to consider the action to qualify as a crime, the usefulness of these data and the reflection of that impairment in the activity of the owner, in addition to the intrinsic value of these own data.

Although it should be noted that when the dimension of the harmful event involving the destruction or impeding of telecommunication facilities be applied art. 560.1 of the Penal Code. As he highlighted M ARCHENA G Omez [46], widespread destruction programs email management must be seen as an act against property of the affected.

The legal right however is much broader than the damaged heritage because not only are the data on the network but also legal security in cyberspace. It is, in my view, a pluriofensivo crime. The best known methods to produce the destruction of the logic elements are viruses [47], Trojan horses [48], sniffers [49], logic bombs [fifty] and worms (*worms)* [51].

8. ADMINISTRATIVE PROTECTION

---

[43] As noted US G onzalez R more than a loophole in previous legislation which had was a poor understanding of the requirement of "physicality" or "materiality" that the material object of criminal damage (for more detail, vine required. G onzalez R US, Juan José, "An approach to criminal treatment ...", op. cit., pp. 138-142.

[44] thus G US onzalez R, Juan José, "The cracking and other cases of computer sabotage" *Legal Studies of Public Prosecutions*

II, CEJAJ, Madrid, 2003, p. 216.

[Four. Five] Cfr. C REMADES G arcia, Javier, "Fraud in financial services *on line ", Legal Studies II Fiscal Ministry,*

Madrid, 2003, pp. 271-272. Similarly in the assessment of damages should take into account the economic value of the hours spent on clean up and rebuild the logical elements and corrupted data, the costs of external companies contracted to carry out these tasks, a quantification of the hours lost as a result of denial of service, etc.

[46] Vine. M ARCHENA G Omez, Manuel, op. cit., 2001, p. 9.

[47] Viruses can be defined as software specifically designed to perform two functions: replicating a computer to another system and placed on computers so that it can destroy or modify programs and data files, interfering with the normal operating system processes (vid. S Neyers, Alfredo, *Fraud and other cyber crimes,*

Management and Production Technologies, SA, Madrid, 1990, 101-105). The high number and variety of them, their extraordinary ability to spread and can cause extensive damage that explains the care and concern they have caused. Real cases and the logical difference technique Trojan horse, vine pumps, worms, and., C Lough, Bryan / M UNGO, Paul,

Pirates chip: computing mafia naked, (trad. Camps, Carme), Ediciones B, Barcelona, 1992, pp. 127 et seq. With a detailed exposition of the birth and development of the phenomenon; criminological data and real cases are also available C ORCOY B IDASOLO, Mirentxu, "criminal protection of computer sabotage. Special consideration of the crimes of damage " *Law: Journal of Spanish legal doctrine, jurisprudence and literature,* No. 1, 1990, pp. 1000-1016 and S ieber, Ulrich, "computer crime: Risk and prevention" *Cybercrime (* coord. Mir Puig, Santiago), 1992, pp. 25-27 "Documentation for an approach to computer crime", op. cit., pp. 74-77.

[48] It is called Trojan Horse (or Trojan), faithful English translation *Trojan horse* though not so used) to a malicious program capable of staying on computers and allow access to external users through a local network or the Internet, in order to gather information or remotely control the host machine. A Trojan is not in itself a virus, even though theoretically can be distributed and function as such. The fundamental difference between a Trojan and a virus is its purpose. For a program to be a "Trojan horse" has only to access and control the host machine without being noticed, usually under a harmless appearance. Unlike a virus, which is a destructive host, the Trojan does not necessarily cause damage because it is not their goal.

[49] The *sniffers* Trackers are programs used to penetrate the hard drive of the computers connected to the network for certain types of information. One launched into cyberspace *Sniffer* collects the e-mails by circulating and enables control and reading. (For details vine. M Oron L ERMA, Esther, op.cit., Pp. 32-33. Different but similar are cookies, small programs that identify each time a user enters an information server and track your preferences, more while *sniffers* content attack cookies are directed to know the continents of information where it goes.

[fifty] They are known as such certain routines or program changes which produce changes, deletions or alterations file system at a later time than that in which they are introduced, when it reaches a certain time or a certain operation is performed. They are similar to the Trojan horse, although the aim pursued with logic bombs is primarily the damage the system or data; although they can also be used to order payments, transferring funds, etc. Experience shows that are preferred by disgruntled employees who schedule their bang for a time when they are no longer in the company (vid procedure., C L OSA Camacho, Luis, op. Cit., Pp. 47-48 ; S Neyers, Alfredo, op cit, pp 113-114....

[51] To learn more about the particular methodology vine. S Neyers, Alfredo, op. cit., pp. 113-114.

To properly understand the computer crimes, as noted S Errano G Omez [52], it must be remembered that the Criminal Code provides for certain legal concepts innuendo operating as regulatory elements, which tend to be integrated by the definitions previously set by the LOPDAT 15/1999 of 13 December on protection of personal data and its implementing regulation (approved by Royal Decree 1720/2007 of 21 December). These elements function as a bridge between criminal and administrative protection.

Said organic law that collects Title VII violations and disciplinary sanctions in particular art. 44.4 pursued as very serious offenses: data collection in misleading or fraudulent, communication or transfer of personal data outside where they are permitted, collect and treat personal data to which referred to in paragraph 2 of Article 7 if not the express consent of the affected; collect and process the data referred to in paragraph 3 of Article 7 when not provided for by law or affected has not expressly consented, or violate the prohibition contained in paragraph 4 of Article 7,

Likewise, Law 34/2002 of 11 July, services of information society and electronic commerce. It covers some extent this loophole especially in Title VII on Offenses and penalties. In turn, the law includes the duty data retention for Internet service providers.

At Community level it is necessary to consider the art. 17 Directive 95/46 / CE safety regulator in the data processing that legislation imposes on States the obligation to establish the technical and organizational measures appropriate to protect personal data from destruction, accidental or unlawful , accidental loss, alteration, disclosure or unauthorized access, particularly when data transmission is being performed within the network.

To ensure the proper functioning of the market electronically in the field of EU Directives 1998/27 / EC of 19 May 2000/31 / EC of 8 June, both the European Parliament and the Council are held.

9. PHYSICAL AND INTERNET CRIMES IN SPACE CONCRETION

The network has a very mutable, cross-border and dynamic pace that is technologically a very complex entity nature. It entails a certain dark side which causes the feeling of "invisibility" of the offenses committed in its midst. As well it is holding H ERRERA M Oreno [53], This latter feature is its raison d'etre in the "relativity of space and computer time," through which "in a playful cyber flicker, the offender is vested with the absolute attributes of timelessness and ubiquity".

This "anonymous" character [54] It causes the victim's sense of helplessness, bordering with homelessness. Contemplating the countless highways of information flowing through the network, he thinks that criminal justice can never take the responsibility for the attack against the victim feels that faces an "invisible" being against whose attacks just have resigned, by which rarely denounce the facts that are given to their detriment. When delictivo- computer attacks are directed against companies or corporations, the "dark figure" of crime finds its reason for being in the "negative publicity" [55]

this means for companies themselves attacked.

---

[52] Vine. S Errano GÓMEZ, Alfonso, *Criminal law. special part,* 8th Ed, Dykinson, Madrid, 2003, p. 267.

[53] Vine. H ERRERA M Oreno, Myriam, "computer fraud in the Spanish criminal law", News *Criminal, no. 39,* Law, Madrid, 2001, pp. 925-964.

[54] M holds Oron L ERMA the anonymous Internet user could be considered as one of the "rights" of "electronic" citizen (cfr. M Oron L ERMA, Esther, op. cit., p. 27).

[55] Vine. A Damski, Andrzej, "Crimes related to the computer network. Threats and Opportunities: A Criminological Perspective " *Five issues in European Criminal Justice: Corruption, Women in the Criminal Justice System, Criminal Policy Indicators, Community Crime and Computer Crime Preventer,* European Institute for Crime Prevention and Control (HEUNI), Helsinki, 1999, pp. 236-237.

Faced with the difficulties that arise in the prosecution of offenses committed by the network, primarily those derived from territorial principle, suggests the application of the theory of ubiquity and can be asserted according to it both jurisdiction instead of the as the action rather than the result (ie without the "transit sites" are taken into account through telematics route, which would be irrelevant). In favor of this ubiquity says court decisions known as the Order of the TS of March 12, 1996.

But this seemingly simple solution conceals numerous problems and difficulties. With the existing experience to date, we can say that the validity of procedural principles regarding the application of criminal law in space, and the classic zeal that most countries have before authorizing a third country to judge a citizen itself, is greatly complicating the prosecution of the crime committed using internet as a medium.

Lege ferenda, postulable seems specializes in such crimes as local courts instruction, considered in isolation, lack of experience, expertise and adequate logistical mechanisms to deal with the complex dynamics criminal network emanating from jurisdiction.

Thus, the difficulties are realized for example when the criminal activity originates from abroad and the result is produced in Spain however; that is, those commonly known as "distance crimes". The claim of the Spanish judicial authorities to understand our country committed such crimes and claim their corresponding prosecution [56] collides with the frequent application of the *theory of ubiquity* by third countries [57], as this is the most favorable to fill the expansive zeal of its jurisdiction [58]. In addition, on many occasions, the most important criminal behavior are made from countries with porous or flexible for certain criminal offenses, which have very limited means, or that have not ratified any extradition treaty legislation.

10. CONCLUSIONS

Cyberspace is a very fertile breeding ground for the transformation not only of the economy and society but also of law in the coming decades, has become its own right in a vital human progress legally. A cyberspace where you can not move without legal certainty significantly decrease the potential of this and the development and social development.

The absence of specific classification of certain cybernetic behavior has led certain authors, supported by the principle of legality *strictu sensu,* to deny the criminal repression of numerous behaviors. It is accepted that under this name fraudulent or culpable actions or omissions are regulated with any relationship in the commission with a computer well, and specifically committed via the Internet.

First, as it maintained F ernandez AND steban [59], the failure of traditional models of protection in the digital environment is clear, since none of them shares the joint characteristics of globality and complete decentralization with the consequent difficulty and sometimes impossibility to control data from the network.

This problem we face has a unique entity that should not be ninguneada. With regard to software, according to the Business Software Alliance and the Software Publishers Association, of the 523 million software used in 1996 worldwide, 225 million, ie almost half, were pirates. This represented, and then a loss of

11.2 trillion.

---

[56] Under the provisions of art. LOPJ 23 corresponds to the Spanish jurisdiction knowledge of the causes for crimes committed in Spanish (...) territory. He also cognizance of the acts described in the Spanish criminal law as crimes, even if they were committed outside the national territory, provided that the act is punishable at the place of execution.

[57] As is known, there are three criteria or theories: a) Activity theory, according to which the offense committed means where the subject performs externally criminal behavior. b) Theory result, according to the same crime is committed where the external result takes place. c) Theory ubiquity, according to her, the crime committed means where is performed the activity or result (Vid. C OBO OF R OSAL, Manuel / V IVES A nton, Thomas manifests S., *Criminal law. part generates* l, Tirant lo Blanch, Valencia, 1999, pp. 209 et seq.).

[58] Combined with the effect of classical principles such as non-delivery of the national citizen, according to which the extradition of nationals is not granted for offenses corresponding to meet the country's courts or the principle of territoriality; according to him, the effectiveness of our criminal law is limited, generally, the national territory.

[59] Vine. F Ernandez E steban, Maria Luisa, *New technologies, internet and fundamental rights,* Mc Graw-Hill, Madrid, 1988, pp. 90 et seq.

This legal vacuum should not be covered, as noted M Oron L ERMA [60], merely by the punitive law. Rightly the author considers that the behavior of hackers can not always be covered by criminal law because it is not admissible were typing as an autonomous crime of mere activity, so it would be wise to contemplate, if any, such conduct outside the criminal system. It examined the various possibilities of the Spanish Penal Code at this point, it is concluded that the conduct of computer intrusion are not always fit into different types.

insufficient rules and administrative mechanisms police penalizing denoted and berate both perpetrators of hacking as network operators and providers providers access services that provide links to default or neglect favor this type of illicit activities .

Moreover conferring the above entities telematic some responsibility, it is not possible to impose either a generic duty control so that the provider becomes a sort of ironclad guarantee of the legality of the contents put on your server by third parties [61].

Alone should intervene Criminal Law when markedly exceed the administrativosancionadora and behaviors that conflict with legal certainty that should govern cyberspace barrier. In other words the repressive legal approach should continue starred primarily by the Administration under the Fragmentary principles and minimum intervention.

Secondly prevention against this type of behavior should have a clear technical dimension, not just legal. So the technology itself tends to react to the risks that unconsciously generates: antivirus programs, cookies cancellers, detectors *web bugs,* repeaters mail (*anonymus remailers),* anonymizer navigation, servers *proxy,* cryptographic applications and software agents or security protocols are examples of this struggle for safeguarding computer privacy.

In analog sense M ORON L ERMA [62] It considers that the implementation of the technical security measures instrumentalized through appropriate technological measures, appears as the most appropriate way having a preferential basis on the criminal threat.

However, this type of autotutela user self-protection or have the serious disadvantage of leaving undefended broad layers of the population who do not have financial or technical resources to ensure their own protection.

Thirdly because cyberspace is projected across national borders an international regulation on this matter is necessary. Computer manipulation performed remote data raises the question of what the applicable law when mismatch rather than manipulation with where the fraudulent result occurs.

The essentially cross-border and international nature of the information highways and the free flow of information that flows from such networks do we meet with a decentralized, globalized and temporarily unlimited spatial parameters. This lack of boundaries avoca us a necessary international cooperation, which should be reflected in both legislative harmonization (as in the case of the European Union) and, in turn, to foster closer judicial and international collaboration.

Finally, it does not seem negligible, by way of *lege ferenda,* encourage the creation of a specialized field of cybercrime jurisdiction. The complication and enormous difficulty involved in instructing such causes do need to download to local courts of their persecution and entrust it to a new curia, proficient and expert in these conflicts, to provide a degree of legal certainty and professionalism that makes the infosphere the old dream of Tim Berners Lee "a place of universal communication chaired by the ideal of freedom and individual autonomy".

---

[60] Vine. M ORON L ERMA, Esther, "Criminal Law and new technologies: current situation and future prospects" *Internet and legal pluralism: emerging forms of regulation, (* coord. by Pompeu Casanovas, Romeo), Comares, Granada, 2003, pp. 93 et seq.

[61] In analog sense ORON M L ERMA, Esther, op. cit., p. 170.

[62] Cfr. M ORON L ERMA, Esther, op. cit., p. 171.

SUPPORTS

1.- ' *phishing* 'Is a phishing pursuing appropriate confidential user data to undermine foreign assets

2.- ' *pharming* 'It is the exploitation of a vulnerable DNS server or user equipment to redirect one domain to another computer

3. One of the main features of computer scam is that structurally is not required deception

4. The manipulation is to alter, modify or hide computer data to improper operation or not are carried out with

5. The *Hacking* It consists of outside unauthorized access to files and databases systems

6. The *'Cracking'* It involves destruction or damage production system, data, software or telematic

7. The victim feels that faces an "invisible" to be against attacks whose only remains resign themselves, so rarely complaint